JH

AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Perlmutter, et al.	Examiner:	D. Duong
Serial No.:	09/740,052	Art Unit:	2663
Filed:	12/19/2000	Attorney Docket No.:	NN-13361
Title:	BANDWIDTH MANAGEMENT FOR TUNNELING SERVERS		

CERTIFICATE OF MAILING

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being deposited with the United States Postal Service as first class mail under 37 C.F.R. 1.8, and is addressed to M.S. Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 10, 2004.

John C. Gorecki, Reg. No. 38,471

M.S. Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

Transmitted herewith is a Reply Brief in the above-identified application. The fee has been calculated and is transmitted as shown below:

	Number of Claims Remaining After Amendment	Highest Number of Claims previously paid for	Number of Extra Claims Present	Rate	Additional Fee
Total Claims	23	23	0	x $18.00	$0
Independent Claims	10	10	0	x 86.00	$0
TOTAL ADDITIONAL FEES FOR THIS AMENDMENT					$0.00

No fees are believed due in connection with this filing. If any additional fees are due in connection with this filing, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref. NN-13361). A duplicate copy of this sheet is enclosed.

Respectfully Submitted

Dated: November 10, 2004

John C. Gorecki
Registration No. 38,471

John C. Gorecki, Esq.
Patent Attorney
180 Hemlock Hill Road
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Perlmutter, et al.	Examiner:	D. Duong
Serial No.:	09/740,052	Art Unit:	2663
Filed:	12/19/2000	Attorney Docket No.:	NN-13361
Title:	BANDWIDTH MANAGEMENT FOR TUNNELING SERVERS		

CERTIFICATE OF MAILING

I hereby certify that this document, along with any other papers referred to as being attached or enclosed, is being deposited with the United States Postal Service as first class mail under 37 C.F.R. 1.8, and is addressed to M.S. Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 10, 2004.

John C. Gorecki, Reg. No. 38,471

M.S. Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

Applicants respectfully submit this Reply Brief in response to the Examiner's Answer dated September 15, 2004. The Examiner's Answer contained a new ground of rejection.

TABLE OF CONTENTS

(1) Real Party In Interest

This application is owned by Nortel Networks, Limited, of St. Laurent, Quebec, CANADA.

(2) Related Appeals and Interferences

None

(3) Status of Claims

Claims 2 and 11 have been canceled.

Claims 1, 3-10, and 12-18 are pending in the application and stand rejected. The rejection of claims 1, 3-10, and 12-18 is being appealed.

(4) Status of Amendments

There are no un-entered amendments.

(5) Summary of claimed subject matter

This invention relates to a method for a server to manage bandwidth of a link not directly connected to the server, to enable differentiate classes of service of traffic to use the link without requiring modification of routers forming a path through the network. (Specification at p. 2, lines 6-7). A VPN server may be disposed within a local area network having very high bandwidth links, such as 100MB links. (Specification at page 4, lines 9-13). The traffic flowing through the VPN server, however, will ultimately be required to contend for a limited amount of bandwidth on a link connected to the Local Area Network by a service provider. (Specification at page 4, lines 13-17). Thus, traffic to be transmitted over the VPN cannot be controlled by the VPN server in a standard fashion since the VPN server may not be connected to the link that is likely to experience congestion. (Specification at page 4, lines 17-20). Applicants discovered that by allowing bandwidth to be metered on a per-application group basis at the VPN server, different application groups could share a link fairly by causing packets within an application group to contend for bandwidth allocated to that application group, and to not contend for bandwidth allocated to other application groups. (Specification at p. 4, line 21 to p. 5, line 4).

There are ten independent claims, of which claims 1, 3, 5, 8, and 9 are similarly drafted independent method claims and claims 10, 12, 14, 17, and 18 are similarly drafted independent apparatus claims. Since the limitations of the method claims are similar, and since the limitations of the apparatus claims are similar, only one claim of each type will be summarized herein.

Independent claim 1 recites a method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link (Specification at page 4, lines 21-25, and Fig. 1, reference numeral 100), comprising: assigning by the VPN server a portion of the bandwidth to at least one application group (Specification at page 4, line 25 to page 5, line 1, page 7, lines 20-21, and Fig. 2); metering by the VPN server packets belonging to the application group (Specification at page 5, lines 1-4, Page 7, lines 22-25, and Fig. 3); wherein the VPN server is configured to at least one of authenticate (Specification at page 1, lines 11-13), encapsulate (Specification at page 1, lines 16-21), and de-encapsulate (Specification at page 2, lines 16-17) at least a portion of the packets.

Independent claim 10 recites a system for managing bandwidth of a remote link comprising: a Virtual Private Network (VPN) server (Specification at page 3, lines 25-28, and Fig. 1, reference numeral 100); a contention pool having a portion of the bandwidth for at least one application group (Specification at page 4, line 25 to page 5, line 4 and Fig. 2); and a meter associated with the VPN server for metering the packets belonging to the application group (Specification at page 7, lines 12-16); wherein the VPN server is configured to at least one of authenticate (Specification at page 1, lines 11-13), encapsulate (Specification at page 1, lines 16-21), and de-encapsulate (Specification at page 2, lines 16-17) at least a portion of the packets.

(6) Grounds of rejection to be reviewed on appeal

Claims 1, 3-10, and 12-18 stand rejected under 35 USC 103 over Ma et al (Ma) (U.S. Patent No. 5,953,338) in view of Jang et al (Jang Utility Application) (U.S. Publication No. 2001/004357A1).

(7) Interview Summary

Prosecution of this application was reopened by the Examiner. In connection with preparing this response, applicants representative conducted two telephone interviews with Examiner D. Duong on October 14, 2004, and October 21, 2004. During the interviews, the newly cited Jang reference was discussed. Specifically, applicant's representative explained that Jang qualified as prior art only due to its priority claim to a provisional application, and also pointed out that the provisional application did not contain the text or figures cited by the Examiner in the rejection. Since the matter relied on by the Examiner was added after applicant's filing date, applicants argued that it could not be relied on by the Examiner in the rejection. The Examiner stated in the second interview that the new matter added to the Jang provisional and first appearing in the published Jang utility application would not be citable against the claims pending in this application, but declined to discuss how that affected the merits of the pending rejection. Applicants have explained the basis and relevance of this argument in greater detail below.

(8) Argument

Rejection under 35 U.S.C. 103 over Ma in view of Jang

The rejection of claims 1, 3-10, and 12-18 under USC 103 over Ma (U.S. Patent No. 5,953,338) in view of Jang (U.S. Publication No. 2001/004357A1) should be reversed because (1) the cited portion of the Jang publication was not disclosed before the filing date of this application – it wasn't part of the Jang provisional application and was only added as new matter to the Jang Utility Application which was filed after the filing date of this application; and (2) A person of ordinary skill in the art would not have found it obvious to modify Ma to include the features of Jang as asserted by the Examiner.

(1) The Cited Portion Of The Jang Publication Was Not Disclosed Before The Filing Date Of This Application.

This application was filed December 19, 2000. Jang filed a provisional application before the filing date of this application and then subsequently filed a utility application after the filing date of this application. Thus, while any subject matter disclosed in the provisional application would be citable against the pending claims of this application, any new matter that was added to the Jang provisional application and first appeared in the Jang Utility Application may not be cited against the claims of this application. Specifically, it is well established that where an applicant seeks to assert priority over a reference, the date of interest in determining priority is the date at which any new matter was introduced into the reference. Specifically, section 715 of the MPEP states:

> "Should it be established that the portion of the patent, or patent application publication, disclosure relied on as the reference was introduced into the patent application by amendment and as such was new matter, the date to be overcome by the affidavit or declaration is the date of amendment."

In this instance, the filing date of the instant application is prior to the filing date of the Jang Utility Application. Thus, any new matter introduced into the Jang Utility Application that was not disclosed in the Jang Provisional Application does not have priority over this application and, hence, may not be cited in a rejection of the claims of this application.

The portion of the Jang patent cited by the Examiner was not included in the Jang Provisional Application

The Examiner cited the Jang Utility Application as disclosing "a data communication system comprising a video conferencing switch 12 (server) comprising a VPN tunneling module 411 configured for authentication, encryption, and compression of packets (Fig. 4A-B page 6, paragraph 0066)." As discussed in greater detail below, these portions of Jang are not contained in the Jang Provisional Application. Additionally, it does not appear that the original Jang Provisional Application disclosed a VPN system but rather disclosed a H.323 gateway. For convenience, a copy of the Jang Provisional Application is attached hereto, which was printed off of the U.S. Patent and Trademark Office's public PAIR site.

The Jang Provisional Application contains two figures, both of which are described at page 1 as "a schematic illustration of an exemplary computer network communications management system." Figs. 4A-4B of the Jang Utility Application, which were cited by the Examiner in this rejection, are not contained in the Jang Provisional Application, and applicant's review of the Jang Provisional Application indicates that reference number 411 and the box to which it refers, is not illustrated or discussed in the Jang Provisional Application. Applicants' representative also reviewed the Jang Provisional Application for a reference to a VPN tunneling module and were not able to find such a reference.

The Jang Provisional Application, for example at page 2, describes a system that works by acting as a high-performance streaming data switch to establish network communications between internal and external streaming applications. The system is later described as having a H.323 gateway. Functions to be performed by the system are described starting at page 2. The described functions include providing a specialized firewall service and proxy service to set up the streaming media calls (page 4, line 4 to page 5, line 9), a Network Address Translation service for streaming data (page 5, lines 10-19), a streaming policy engine that provides fine-grained policies for managing the security and network bandwidth utilization for streaming traffic (page 5, line 20 to page 6, line 17), and a QoS service for streaming data (page 6, line 18-page 8, line 2). The system also incorporates a streaming data encryption module and a bandwidth management module. (page 8, lines 3-13).

The Jang Provisional Application, doesn't describe the system as being a VPN server, but rather describes it as a H.323 gateway. Specifically, the Jang Provisional Application teaches that the system should use a H.323 proxy/gatekeeper to enable secure incoming and outgoing call resolution. For example, whereas applicant's representative was unable to find any reference to a VPN server, the Jang Provisional Application mentions H.323 at least 8 times, for example at page 4, line 8; page 4, line 12; page 5, line 2 (twice); page 5, line 16; page 6, line 3; page 9, line 20; and on page 21, a slide entitled VideoIP™ 8000 Features.

As is well known, H.323 is a call setup protocol that allows videoconferencing and other communications such as voice to take place over a packet-based network. The Jang Provisional Application references to security and policy are all consistent with this interpretation – note that version 4 of the H.323 protocol was released in 2000, and many if not all of the functions to be performed by the system described in the Jang provisional were supported by version 4 of the H.323 protocol. Thus, the Jang Provisional Application does not disclose a VPN server but rather discloses a H.323 gateway that may be used to support streaming media across a firewall.

(2) A Person Of Ordinary Skill In The Art Would Not Have Found It Obvious To Modify Ma To Include The Features Of Jang As Asserted By The Examiner.

As set forth in applicant's recently filed Appeal Brief, the content of which is hereby incorporated herein by reference, this application relates to a method and apparatus configured to allow a VPN server to manage the bandwidth of a link that is not directly connected to the server. This may be useful, for example, where the VPN server is connected to high bandwidth local area network links and the VPN traffic it is handling will ultimately be required to be passed out of the LAN over a relatively lower bandwidth external link. (See Specification at page 4, lines 9-20). Allowing the bandwidth of the link to be managed at the VPN server enables traffic with different class of service priority to use the lower bandwidth link without requiring modification of routers forming a path through the network. (Specification at p. 2, lines 6-7). Further, by allowing bandwidth to be metered on a per-application group basis, different application groups can share a link fairly by causing packets within an application group to contend for bandwidth allocated to that application group, and to not contend for bandwidth allocated to other application groups. (Specification at p. 4, line 21 to p. 5, line 4).

The Examiner has taken the position that Ma discloses a system for managing bandwidth of a remote link in a VPN 170 (Ma at Fig. 1) comprising a server 160 (Ma at Fig. 2, Col. 7 lines 5-14), a contention pool 401 or 402 having a portion of the bandwidth for at least one application group (Ma at Fig. 4A Col. 11 lines 11-26) and a meter 145 for metering the packets belonging to the application group. The Examiner admits that Ma fails to teach that the server is a VPN server configured to authenticate, encapsulate or de-encapsulate at least a portion of the packets, but contends that Jang discloses a video conferencing switch 12 comprising a VPN tunneling module 411 configured for authentication, encryption, and compression of packets, citing Jang at page 6, paragraph 0066 and Fig. 4A-B) (Office Action at page 3). Thus, the Examiner concludes that it would have been obvious to combine Jang with Ma to provide this added functionality to the server in Ma.

The server in Ma is a central server, and not a VPN server as admitted by the Examiner. More specifically, the server 160 in Ma is a "centralized control module" that interfaces with ATM edge switches 130A, 130B, ... 130F to control each individual ATM edge switch. In so doing, the centralized control module 160 "controls the creation and nature of virtual paths and virtual channels extending throughout the overall ATM Network 120 (in FIG. 1B). (Ma at Col. 6, lines 57-63). Thus, Ma does not handle packets on the links. In fact, since it is a centralized control, it cannot handle packets on the links that it is monitoring.

Additionally, Ma enforces implementation of the bandwidth metering by modifying the operation of the ATM switches. By contrast, as discussed above, the instant invention allows a VPN server to manage the bandwidth of a remote link without requiring modification of routers forming a path through the network. (Specification at p. 2, lines 6-7). Thus, the operational principal of Ma is opposite that of the instant invention.

The Examiner has cited Jang as teaching a video conferencing switch 12 comprising a VPN tunneling module 411 configured for authentication, encryption, and compression of packets, citing Jang at page 6, paragraph 0066 and Fig. 4A-B) (Office Action at page 3). Even if Jang is citable with respect to this material, applicants respectfully submit that a person of ordinary skill in the art would not have been motivated to modify Ma to include this functionality, as suggested by the Examiner for one simple reason – Ma doesn't handle packets. Since Ma doesn't handle packets it wouldn't have been obvious to add functionality to handle the packets in a different manner. Additionally, the manner in which Ma effects control over bandwidth (by modifying routers on the path) is opposite the manner in which the present invention effects control over bandwidth on the links (by metering packets). Thus, a person of ordinary skill in the art would not have been motivated to modify the manner in which Ma operates to cause Ma to authenticate, encapsulate, or deencapsulate packets, since the server in Ma doesn't handle the packets that may benefit from one or more of these services.

Independent Claim 1

Independent claim 1 recites a method for a VPN server that manages bandwidth of a remote link, comprising assigning a portion of the bandwidth to at least one application group, and metering by the VPN server packets belonging to the application group. Claim 1 further recites that the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets. Thus, the VPN server in independent claim 1 manages bandwidth of a remote link by doing three things: (1) it assigns bandwidth of the remote link to an application group; (2) it meters packets belonging to the application group; and (3) it authenticates, encapsulates, or de-encapsulates the packets that belong to the application group on the link that is being metered. Since it would not have been obvious to modify Ma to perform this method, the rejection of claim 1 should be reversed.

Independent Claims 3, 5, 8, and 9

Independent claims 3, 5, 8, and 9, contain limitations similar to the combination of limitations discussed above in connection with claim 1. Accordingly, independent claims 3, 5, 8, and 9 are patentable for at least the same reasons set forth above.

Dependent claims 4, 6, and 7

Dependent claims 4, 6, and 7 are patentable for at least the same reasons as their respective independent claim.

Independent Claims 10, 12, 14, 17, and 18

Independent claim 10 recites a system for managing bandwidth of a remote link, comprising: a VPN server, a meter associated with the VPN server for metering packets belonging to the application group, and that the server is a VPN server configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the metered packets. As discussed above, the combination of Ma and Jang fails to teach or suggest a system of this nature. Although the arguments have been presented with respect to method claim 1, they apply equally to independent apparatus claim 10. Accordingly, independent claim 10 and similarly drafted independent claims 12, 14, 17, and 18 are patentable over the combination of Ma and Jang.

Dependent claims 13, 15, and 16.

Dependent claims 13, 15, and 16 are patentable for at least the same reasons as their respective independent claim.

(9) Conclusion

Applicants respectfully submit that the claims pending in this application are in condition for allowance and respectfully request that the rejection of the claims be reversed.

No fees are believed due in connection with this filing. If any fees are due, the Commissioner is hereby authorized to charge payment of the fees associated with this communication or credit any overpayment to Deposit Account No. 502246 (Ref: NN-13361).

Respectfully Submitted

Dated: November 10, 2004

John C. Gorecki
Registration No. 38,471

John C. Gorecki, Esq.
Patent Attorney
180 Hemlock Hill Road
Carlisle, MA 01741
Tel: (978) 371-3218
Fax: (978) 371-3219
john@gorecki.us

APPENDIX A – PENDING CLAIMS

1. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group; and

metering by the VPN server packets belonging to the application group;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

2. Canceled

3. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group; and

metering by the VPN server packets belonging to the application group;

wherein the VPN server is directly connected to other links having larger bandwidth than the available bandwidth of the remote link; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

4. The method of claim 1 wherein the packets belonging to the application group share a pre-defined configuration.

5. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group; and

metering by the VPN server packets belonging to the application group;

wherein the packets belonging to the application group contend equally for the portion of the bandwidth; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

6. The method of claim 1 wherein metering the packets group further includes metering flow rate of the packets going through the server in either direction.

7. The method of claim 6 wherein metering the packets further includes rejecting the packets if the flow rate exceeds the portion of the assigned bandwidth.

8. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group;

metering by the VPN server packets belonging to the application group; and

allowing a user to specify the bandwidth of the remote link from a user interface;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

9. A method for a Virtual Private Network (VPN) server that manages bandwidth of a remote link, comprising:

assigning by the VPN server a portion of the bandwidth to at least one application group;

metering by the VPN server packets belonging to the application group; and

allowing a user to specify the portion of the assigned bandwidth from a user interface;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

10. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering the packets belonging to the application group;

wherein the server is a VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

11. Canceled

12. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and a meter associated with the VPN server for metering packets belonging to the application group by the VPN server;

wherein the VPN server is directly connected to other links having larger bandwidth than the available bandwidth of the remote link; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

13. The system of claim 10 wherein the packets belonging to the application group share a pre-defined configuration.

14. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server;

wherein the packets belonging to the application group contend equally for the contention pool; and wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

15. The system of claim 10 wherein the meter further meters flow rate of the packets going through the server in either direction.

16. The system of claim 15 wherein the meter further rejects the packets if the flow rate exceeds the assigned portion of the bandwidth.

17. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server; and

a user interface that allows a user to specify the bandwidth of the link;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

18. A system for managing bandwidth of a remote link comprising:

a Virtual Private Network (VPN) server;

a contention pool having a portion of the bandwidth for at least one application group; and

a meter associated with the VPN server for metering packets belonging to the application group by the VPN server; and

a user interface that allows a user to specify the assigned portion of the bandwidth;

wherein the VPN server is configured to at least one of authenticate, encapsulate, and de-encapsulate at least a portion of the packets.

APPENDIX B – EVIDENCE

None.

APPENDIX C – RELATED PROCEEDINGS

None.